FORTINET

High Performance Network Security

FortiMail™ Release Notes

VERSION 6.0.0 GA

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

June 01, 2018

TABLE OF CONTENTS

Change Log

Date	Change Description
2018-05-25	Initial release.
2018-06-01	Updated upgrade path. Changed “5.4.4 (Build 714) (Required for VM install only)” to “5.4.4 (Build 714) (Required for VMware install only).

Introduction

This document provides a list of new and changed features, upgrade instructions and caveats, resolved issues, and known issues in FortiMail 6.0.0 release, build 0091.

Supported Platforms

- FortiMail 60D
- FortiMail 200D
- FortiMail 200E
- FortiMail 400E
- FortiMail 1000D
- FortiMail 2000E
- FortiMail 3000D
- FortiMail 3000E
- FortiMail 3200E
- FortiMail VM (VMware vSphere Hypervisor ESX/ESXi 5.0 and higher)
- FortiMail VM (Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2)
- FortiMail VM (KVM qemu 0.12.1 and higher)
- FortiMail VM (Citrix XenServer v5.6sp2, 6.0 and higher)
- FortiMail VM [AWS(BYOL)]
- FortiMail VM [Azure(BYOL)]

What's New

The following table summarizes the new features and enhancements in this release.

Features	Descriptions
URI click protection	When a user clicks a URI in the email message, the URL will be directed to the FortiMail device for additional FortiGuard URI Filter service scanning. Enterprise ATP license is required.
Impersonation analysis	Guards against email impersonation attacks by mapping display names with email addresses. Enterprise ATP license is required.
Email delivery control	Rate limits email delivery in ACL policies.
LDAP ACL verification	Queries the LDAP server to verify individual sender and recipient.
Network interface access control	Adds web access and mail access control to individual network interfaces.
Authentication reputation	Tracks and scores login attempt failures to mitigate the risk of password guess attacks.
FortiView support	Adds FortiView support to admin GUI.
Email subject scan	Adds DLP sensitive data scanning and URI checking to email subject.
Decrypt password protected Office document	Adds Office document decryption support in content profiles.
SAML SSO and Google G-Suite integration	Third party SSO support is added under System > Customization > Appearance > Web Portal.
NTLM support	Supports NTLM authentication in relay host setting and domain settings.
Acceptable client certificate CA names	Adds a new CLI command (config system mailserver : set show-acceptable-cert-ca : enable | disable) to enable/disable “Acceptable client CA names” during TLS handshake.
SHA256 file signatures	Adds support under Security > Other > File Signature.
IBE password reset page customization	Adds support to customize IBE password reset page and login page under System > Customization > Custom Message.
Relay types	Adds support to configure relay types (host, MX record, and IP group) under System > Mail Settings > Relay Host List. Only host type was supported before.
Cross search in mail queue and system quarantine	Adds cross search with session ID in mail queue and system quarantine. After clicking on the session ID, all related messages will be displayed.
SSL Cipher configuration	Added CLI commands (under config system security crypto) to separately configure SSL ciphers for mail and web access.

Features	Descriptions
Security Fabric	FortiMail statistics can be viewed from the FortiOS GUI as part of the Security Fabric integration.

What's Changed

The following table summarizes the behavior changes and GUI reorganizations in this release.

Features	Descriptions
Dashboard reorganization	Some dashboard items are moved to FortiView menu.
Stong-crypto	Strong-crypto is enabled by default starting from 6.0 release. Because some old versions of email clients (for example, MS Outlook 2007 and older) and MTAs only support TLS 1.0, they may have issues connecting to FortiMail. To fix the issue, use CLI command “config system security crypto” to disable strong-crypto and add TLS 1.0 support. For details, see FortiMail CLI Reference.
Hard limit enforcement	On some models, there used to be soft limits on the maximum number of domains, associated domains, and mail users. Now the soft limits are removed and hard limits are enforced.
Automatic backup	Automatically back up configuration when installing firmware image or restoring configuration from a configuration file.
Key management	Enhanced password encryption and key management.
Attachment names in notification message	Lists all attachment names in notification email. Only the first attachment name was included before.
Millisecond timestamp	Adds millisecond timestamp in all logs.
Web access	Access to the Admin GUI and Webmail can be configured on a per interface basis.
Licensing changes	The licensing model has been changed to accommodate the new features added in the 6.0.0 release. Two new bundles are now available: **Base Bundle**: Includes 24x7 FortiCare Support, FortiGuard AV, AS, and Virus Outbreak Service, Identity Based Encryption, Data Loss Prevention, and archiving. **Enterprise ATP Bundle**: Includes 24x7 FortiCare Support and all of the Base Bundle features as well as FortiCloud Sandbox, Content Disarm and Reconstruction (CDR), URI Click Protection, Business Email Compromise (Impersonation Analysis).

Special Notices

TFTP firmware install

Using TFTP via the serial console to install firmware during system boot time will erase all current FortiMail configurations and replace them with factory default settings.

Monitor settings for web UI

To view all objects in the web UI properly, Fortinet recommends setting your monitor to a screen resolution of at least 1280x1024.

Recommended browsers on desktop computers for administration and Webmail

- Internet Explorer 11 and Edge 40, 41
- Firefox 52.7.2 ESR, 59
- Safari 10, 11
- Chrome 65

Recommended browsers on mobile devices for Webmail access

- Official Safari browser for iOS 10, 11
- Official Google Chrome browser for Android 6.0 to 8.0

FortiSandbox support

- FortiSandbox 2.3 and above

SSH connection

For security reasons, starting from 5.4.2 release, FortiMail stopped supporting SSH connections with plain-text password authentication. Instead, challenge/response should be used.

Firmware Upgrade/Downgrade

Before and after any firmware upgrade/downgrade

- Before any firmware upgrade/downgrade, save a copy of your FortiMail configuration (including replacement messages) by going to *System* > *Maintenance* > *Configuration*.
- After any firmware upgrade/downgrade:
  - If you are using the web UI, clear the browser cache prior to login on the FortiMail unit to ensure proper display of the web UI screens.
  - The antivirus signatures included with an image upgrade may be older than those currently available from the Fortinet FortiGuard Distribution Network (FDN). Fortinet recommends performing an immediate AV signature update as soon as possible.

Upgrade path

For any 5.x release

Any 5.x release older than 5.2.3
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
6.0.0 (Build 0091)

For any 4.x release

Any 4.x release older than 4.3.6
↓
4.3.6 (Build 540)
↓
5.2.3 (Build 436)
↓
5.2.8 (Build 467)
↓
5.3.10 (Build 643)
↓
5.4.4 (Build 714) (Required for VMware install only)
↓
6.0.0 (Build 0091)

After every upgrade, verify that the build number and branch point match the image that was loaded by going to *Dashboard* > *Status* on the Web UI.

Firmware downgrade

Downgrading from 6.0.0 to 5.x or 4.x releases

Downgrading from 6.0.0 release to any 5.x or 4.x release is not fully supported. If you have to downgrade, follow these steps:

1. Back up the 6.0.0 configuration.
2. Install the older image.
3. In the CLI, enter `execute factoryreset` to reset the FortiMail unit to factory defaults.
4. Configure the device IP address and other network settings.
5. Reload the backup configuration if needed.

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Antivirus/Antispam/Content

Bug ID	Description
477064	Some rescan email is released before FortiSandbox verdict.
471131	Recipient outbound policies with protected domain as sender pattern are not triggered when email is sent from webmail.
482917	When decrypting PDF files, the mailfilterd daemon may crash in some cases.
474861	HTML content is not converted to text even though this feature is enabled in the content profile.
490887	FortiMail should combine base and relative URL against baseStriker attacks.
490890	When email re-scan is on, quarantined messages cannot be released in some cases.
468197	After enabling "Safelist recipients of outbound message" in a resource profile and "Enable Outgoing Recipient Safelisting" in user preferences, the automatic safelisting works only for the current view.
480189	PDF files with embedded script enabled cannot be detected by content profiles after antivirus scan.
486092	FortiGuard Web Filter Service identifies URI: http://www.amazon.com as Newly Observed Domain, instead of Shopping category.
477659	DKIM signatures are inserted twice if the outbound email is inspected by FortiSandbox.
484358	An email message which is deferred for both spam outbreak and FortiSandbox URI scanning will be delivered when the spam outbreak expires without waiting for FortiSandbox scan results or timeout.
479590	Email attachment file size is calculated incorrectly.
476336	Quarantine report email cannot be displayed properly after the template is modified.
491705	When the default action is selected in the recipient policy, email for an unknown user cannot be found in system quarantine although the log message disposition says so.

Mail Receiving and Delivering

Bug ID	Description
474266	Email is sent to a server defined in a routing profile after a few delivery tries.
477351	Cannot reach the relay host using FQDN.
470130	IBE encryption using Access Control Delivery rules always matches wildcard domains instead of more specific recipients.
474627	When disclaimer is inserted, some incoming email body is displayed as attachment in Outlook.

Bug ID	Description
484700	Email body is cut off when enabling incoming disclaimer at the start of message.
485716	Delivery receipt with S/MIME signing does not work.
489283	Returned mail contains incorrect From address when one of the recipient address cannot be reached.
475042	Session profile advanced mail routing to MX record of alternative domain does not work.

System

Bug ID	Description
476741 476780	Hardens password encryption.
478518	For PCI compliance, SSL and TLS 1.0 should not be enabled by default.
480291	CVE-2017-14461 DoveCot Information Leak Vulnerability.
471556	After upgrading from 5.4.2 to 5.4.4, the rotated quarantine folders cannot be opened.
475724	After upgrading to 5.4.4 release, the CPU usages reaches 100%.
480712	When the email archive account disk quota is full, the previously rotated folders will be deleted.
475348	FortiGuard antispam override IP address is not used if it is a public address.
483796	When setting up LDAP address book mapping under Domain & User > Address Book > LDAP Mapping, some contact fields are missing in 5.4 releases compared with 5.3 releases.
488513	When a FortiMail DNS query response is SERVFAIL, the secondary DNS server is not queried.
476356	RADIUS users cannot be imported by using CSV files.
472457	Internal Server Error occurs when downloading PKCS12 file of certification which status is pending.
475337	Admin profile changes are not synchronized to the HA slave unit.
409777	Some system events SNMP traps are not sent.
490889	If FortiMail uses the “exe ssh” command to connect to other server and the server changed its SSH key, the connection will fail with a warning.
483185	In HA mode, VIP does not work for the Redundant interface with a long interface name.
481223	The status of IBE security questions is not retained after firmware upgrade.
480951	High CPU usage due to mailfitlerd processes.
469984	Additional HTML tags are inserted in disclaimers.
477122	Multiple mailfitlerd crashes.

Bug ID	Description
484202	CSR download button is greyed out under System > Certificate > Local Certificate.
480659	Return-path in mail header is removed after email migration from other mail servers.
479310	Unable to add email addresses containing single quotes into email address groups.
489047	Admin users without system privileges can change the system time.
478702	The mailfilterd process causes high CPU usage.
490052	Wrong certificate chain is supplied when an IP pool is used.
490548	Importing LDAP contacts does not skip the already existing ones and thus create duplicates.

Log and Report

Bug ID	Description
469409	CRLF is not displayed properly by SPF check in logs.
475040	In some cases, report generation may stop when Daylight Saving Time starts.
475545	Non-US-ASCII logs sent to FortiAnalyzer are not searchable.
489533	Week numbers in FortiMail reports are not displayed correctly.

Admin GUI/Webmail

Bug ID	Description
477852	With Internet Explorer and Edge, the empty Calendar Resource table is not displayed properly in webmail.
477882	The Compose button is missing for internal IBE users in webmail.
472978	Cyrillic characters are not displayed properly in quarantine preview.
473566	When FortiMail VM cannot access the Internet, a meaningless message is displayed.
472967	Under System > Maintenance > Mail Data > Backup Options, the “Initiator name as username” option should not appear when iSCSI Server is not selected.
474405	Under Security > Bayesian > Domain, the Bayesian database cannot be restored.
472469	Bridge should not be selectable on virtual IP action of HA configuration when the operation mode is server or gateway.
470864	Japanese translation of “Instant Message” is wrong on the View/Edit Contact page in webmail.
469367	Japanese translation of AOL Instant Messenger (AIM) is wrong on the View/Edit Contact page in webmail.
469887	Russian characters for system spam resource key may cause the webmail inaccessible.

Bug ID	Description
485953	The Allow user to change theme option under System > Customization > Appearance > Webmail Portal does not take effect.
482891	IP address and port number combination is not accepted for FDS override IP address under System > FortiGuard > Antivirus.

CLI

Bug ID	Description
486757	The diagnose command: diagnose hardware deviceinfo nic does not work.

Known Issues

The following table lists some minor known issues. .

Bug ID	Description
307919	Webmail GUI for IBE users displays a paper clip for all email although the email has no attachments.
381511	IBE messages are not signed with DKIM although DKIM signing is enabled.

Image Checksums

To verify the integrity of the firmware file, use a checksum tool and compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for Fortinet software and firmware releases are available from Fortinet Customer Service & Support. After logging in to the web site, near the bottom of the page, select the *Firmware Image Checksums* button. (The button appears only if one or more of your devices have a current support contract.) In the File Name field, enter the firmware image file name including its extension, then select *Get Checksum Code*.

Figure 1: Customer Service & Support image checksum tool